United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Monday,
September 11, 2000

COMPUTER SECURITY

Critical Federal Operations and Assets Remain at Risk

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-314

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 11092000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Computer Security: Critical Federal Operations and Assets Remain at Risk	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) GAO	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 20	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/11/00	Report

4. TITLE AND SUBTITLE
Computer Security: Critical Federal Operations and Assets Remain at Risk

5. FUNDING NUMBERS

6. AUTHOR(S)
GAO

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The report released today July 28, 2000, summarizes the results of recent information security audits performed by GAOand by agency inspectors general at 24 major federal departments and agencies.1 In summarizing these results, they discuss the pervasive weaknesses that continue since we reported on the results of a similar analysis 2 years ago this month.2 The report then illustrates the serious risks that these weaknesses pose at selected individual agencies. Finally, It describes the major common weaknesses that agencies need to address in order to improve their information security programs.

14. SUBJECT TERMS
Information Security

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our analysis of recent information security audits at federal agencies. As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of confidential information.

The report being released at today's hearing responds to your July 28, 2000, request that we summarize the results of recent information security audits performed by us and by agency inspectors general at 24 major federal departments and agencies.[1] In summarizing these results, I will discuss the pervasive weaknesses that continue since we reported on the results of a similar analysis 2 years ago this month.[2] I will then illustrate the serious risks that these weaknesses pose at selected individual agencies. Finally, I will describe the major common weaknesses that agencies need to address in order to improve their information security programs.

Background

Dramatic increases in computer interconnectivity, especially in use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of other individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. Telecommunications, power distribution, national defense—including the military's warfighting capability, law enforcement, government services, and emergency services all depend on the security of their computer

[1] *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

[2] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

operations. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Disruptions caused by recent virus attacks, such as the ILOVEYOU virus this past May and 1999's Melissa virus, have illustrated the potential for damage that such attacks hold.[3] In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, or degrade the integrity of and deny access to data. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood that information attacks will threaten vital national interests increases.

Our previous analyses have shown that federal agency systems were not being adequately protected from these threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September 1996, we reported that serious weaknesses had been found at 10 of the largest 15 federal agencies.[4] In that report we concluded that poor information security was a widespread federal problem with potentially devastating consequences; accordingly, in 1997 and 1999 reports to the Congress, we identified information security as a high-risk issue.[5] In 1998, we analyzed

[3] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000). *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000). *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

[4] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

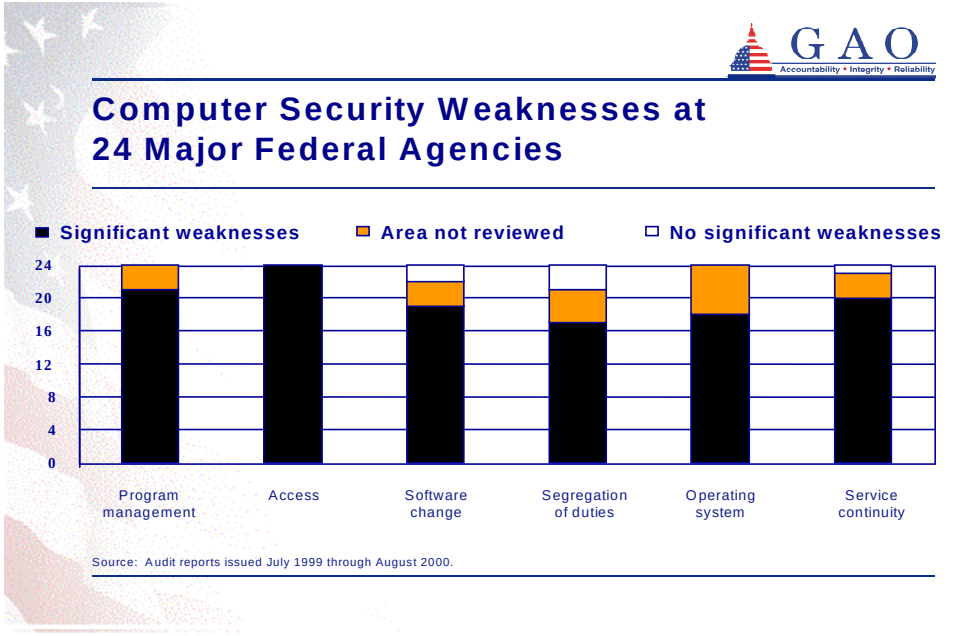
[5] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997). *High-Risk Series: An Update* (GAO/HR-99-1, January 1999).

audit results for 24 of the largest federal agencies: all of them had significant information security weaknesses.[6]

Weaknesses Remain Pervasive

Evaluations published since July 1999 continue to show that federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk. As in 1998, our current analysis identified significant weaknesses in each of the 24 agencies covered by our review. More areas have been reviewed at more agencies and, as in 1998, weaknesses were reported in all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These weaknesses placed a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they placed an enormous amount of highly sensitive data—much of it pertaining to individual taxpayers and beneficiaries—at risk of inappropriate disclosure.

Figure 1: Computer Security Weaknesses at 24 Major Federal Agencies



[6]GAO/AIMD-98-92, September 23, 1998.

Figure 1 illustrates the distribution of weaknesses across the 24 agencies. As in 1998, the most widely audited area, and the area where weaknesses were most often identified, was access controls. Weak controls over access to sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

At 21 of the 24 agencies, problems were also identified in the area of security program management—an area that is fundamental to the appropriate selection and effectiveness of the other categories of controls. Security program management covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

One notable change since September 1998 is that the scope of audit work performed has expanded to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. While these increases in reported weaknesses are disturbing, they do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the numbers leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 1 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at other agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits used to develop the figure may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluating systems supporting nonfinancial operations. In response to congressional interest, during fiscal years 1999 and 2000, we expanded our audit focus to cover a wider range of nonfinancial operations, a trend that is likely to continue.

Risks to Federal Operations, Assets, and Confidentiality Are Substantial

To fully understand the significance of the weaknesses summarized in figure 1, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high. Examples of the significant risks posed to critical federal operations are described below.

- The Department of the Treasury (which includes the Internal Revenue Service; U.S. Customs Service; Bureau of the Public Debt; Financial Management Service; and Bureau of Alcohol, Tobacco, and Firearms) relies on computer systems to process, collect or disburse, and account for over $1.8 trillion in federal receipts and payments annually. Its computers handle enormous amounts of highly sensitive data associated with taxpayer records, law enforcement operations, and support operations critical to financing the federal government, maintaining the flow of benefits to individuals and organizations, and controlling imports and exports. Although protecting these operations and assets is essential, Treasury's Inspector General (IG) reported in February the absence of effective general controls over computer-based financial systems at certain Treasury components, and that this absence of controls made the department vulnerable to losses, fraud, delays, and interruptions in service.[7]

- The Department of Defense (DOD) relies on a complex computerized information infrastructure to support virtually all aspects of its operations, including strategic and tactical operations, weaponry, intelligence, and security. Evaluations of the security of DOD systems since July 1999 have continued to identify weaknesses that could seriously jeopardize operations and compromise the confidentiality, integrity, or availability of sensitive information. In August 1999, we reported that serious weaknesses in DOD information security continued to provide both hackers as well as hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data.[8] As a result, numerous DOD functions—including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll—had already been

[7] *Report on the Department of the Treasury's Fiscal Year 1999 Financial Statements* (OIG-00-056, February 29, 2000).

[8] *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999)

adversely affected by system attacks or fraud. This past May, we testified that the preliminary results of a recent review of the department's financial management systems showed that serious weaknesses in access controls and systems software continued to exist.[9]

- Information technology is essential to the Department of Energy's (DOE) scientific research mission, which is supported by a large and diverse set of computing systems, including very powerful supercomputers located at DOE laboratories across the nation. In June, we reported that computer systems at DOE laboratories supporting civilian research had become a popular target of the hacker community, with the result that the threat of attacks had grown dramatically in recent years.[10] Further, because of security breaches, several laboratories had been forced to temporarily disconnect their networks from the Internet, disrupting the laboratories' ability to do scientific research for up to a full week on at least two occasions.

- In February, the Department of Health and Human Services' (HHS) IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[11] Most significant were weaknesses associated with the department's Health Care Financing Administration, which was responsible, during fiscal year 1999, for processing health care claims for over 39.5 million beneficiaries and outlays of $299 billion—17.5 percent of total federal outlays.

- The Social Security Administration (SSA) relies on extensive information processing resources to carry out its operations, which for 1999 included payments that totaled $410 billion to more than 50 million beneficiaries, many of whom rely on the uninterrupted flow of monthly payments to meet their basic needs. This represents about 25 percent of the $1.7 trillion in federal expenditures. The agency also issues social security numbers and maintains earnings records and other personal information on virtually all U.S. citizens. The public depends on SSA to protect trust fund revenues and assets from fraud and to protect sensitive information on individuals from inappropriate disclosure. According to SSA, no other

[9] *Department of Defense: Progress in Financial Management Reform* (GAO/T-AIMD/NSIAD-00-163, May 9, 2000)

[10] *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/AIMD-00-140, June 9, 2000).

[11] *Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1999*, A-17-99-00002, February 2000.

public program or public-service entity directly touches the lives of so many people.

In November 1999, the IG reported that SSA's systems environment remained threatened by weaknesses in several components of its information protection control structure.[12] According to the IG, until corrected, these weaknesses will continue to increase the risks of unauthorized access to, modification, or disclosure of sensitive SSA information. These, in turn, increase the risks that data or SSA Trust Fund resources could be lost and that the privacy of information associated with SSA's enumeration, earnings, retirement, and disability processes and programs could be compromised. For example, such weaknesses might allow an individual or group to fraudulently obtain payments by creating fictitious beneficiaries or increasing payment amounts. Similarly, an individual or group might secretly obtain sensitive information and sell or otherwise use it for personal gain.

- The Environmental Protection Agency (EPA) relies on its computer systems to collect and maintain a wealth of environmental data under various statutory and regulatory requirements. EPA makes much of its information available to the public through Internet access in order to encourage public awareness and participation in managing human health and environmental risks and to meet statutory requirements. EPA also maintains confidential data from private businesses, data of varying sensitivity on human health and environmental risks, financial and contract data, and personal information on its employees. Consequently, EPA's information security program must accommodate the often competing goals of making much of its environmental information widely accessible while maintaining data integrity, availability, and appropriate confidentiality. In July, we reported serious and pervasive problems that essentially rendered EPA's agencywide information security program ineffective.[13] Our tests of computer-based controls concluded that the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses.

  Of particular concern was that many of the most serious weaknesses we identified—those related to inadequate protection from intrusions through the Internet and poor security planning—had been previously reported to

[12] *Social Security Accountability Report for Fiscal Year 1999*, November 18, 1999.

[13] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215, July 6, 2000).

EPA management in 1997 by EPA's IG.[14] The negative effects of such weaknesses are illustrated by EPA's own records, which show several serious computer security incidents since early 1998 that have resulted in damage and disruption to agency operations. As a result of these weaknesses, EPA's computer systems and the operations that rely on these systems were highly vulnerable to tampering, disruption, and misuse from both internal and external sources.

- In July the Department of Transportation's (DOT) IG reported that reviews of a financial system and 13 network systems identified a general lack of background checks on contractor personnel and a lack of appropriate background checks on employees throughout DOT.[15] The IG also found that the department's systems were vulnerable to unauthorized access by Internet users. Further, in December 1999, we had reported that DOT's Federal Aviation Administration was not following sound personnel security practices and, as such, had increased the risk that inappropriate individuals may have gained access to its facilities, information, or resources.[16] For example, no background searches were performed on 36 mainland Chinese nationals who reviewed the source code of eight mission-critical systems.

- The Department of Veterans Affairs (VA) relies on a vast array of computer and telecommunications systems to support its operations and to store sensitive information the department collects in carrying out its mission. Such operations include financial management, health care delivery, and benefits payments. In September 1998, we reported weaknesses that placed the systems that support these operations at risk of misuse and disruption.[17] In October 1999, we reported that VA systems continued to be vulnerable to unauthorized access.[18] These weaknesses placed sensitive information, including financial data and sensitive veteran medical data and benefit information, at increased risk of inadvertent or

[14] *EPA's Internet Connectivity Controls,* Office of Inspector General Report of Audit (Redacted Version), September 5, 1997.

[15] *Interim Report on Computer Security* (FI-2000-108, July 13, 2000).

[16] *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, December 23, 1999).

[17] *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-98-175, September 23,1998).

[18] *Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 4,1999).

deliberate misuse, fraudulent use, improper disclosure, or destruction—possibly occurring without detection.

- In July 1999, we reported that the Department of Agriculture's National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent or detect unauthorized changes to payroll and other payment data or computer software.[19] NFC is responsible for processing billions of dollars in payroll payments for hundreds of thousands of federal employees and maintaining records for the world's largest 401(k)-type program.

We have made numerous recommendations to the agencies, and in many cases, corrective actions are underway.

While Nature of Risk Varies, Control Weaknesses Across Agencies Are Strikingly Similar

The nature of agency operations and the related risks vary. However, striking similarities remain in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations—and therefore on what corrective actions they must take. The sections that follow describe the six areas of general controls that are represented in figure 1—and the specific weaknesses that were most widespread at the agencies covered by our analysis.

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than react to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Of the 21 agencies for which this aspect of security was reviewed, all had deficiencies. Specifically, many had not developed security plans for major systems based on risk, had not documented security policies, and had not implemented a program for testing and

[19] *USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-99-227, July 30, 1999).

evaluating the effectiveness of the controls they relied on. As a result, agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on controls that were not effective, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require users to authenticate themselves through the use of secret passwords or other identifiers and limit the files and other resources that an authenticated user can access and the actions that he or she can execute. Without adequate access controls, unauthorized individuals, including outside intruders and terminated employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Even authorized users can unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and to keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and terminated employees, and changes in users' responsibilities and related access needs.

Access controls were evaluated at all 24 of the agencies covered by our analysis, and significant weaknesses were reported for each of the 24, as evidenced by the following examples:

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled; neither were they adjusted for those whose responsibilities, and thus need to access certain files, changed. At one agency, as a result, former employees and contractors could and in many cases did still read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.

- Users were not required to periodically change their passwords.

- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At another agency, 20,000 users had been provided access to one system without written authorization.

- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.

- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the capability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate penetration testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. As we reported in 1998, our auditors have been

successful, in almost every test, in readily gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. At one agency, much of the activity associated with our intrusion testing was not recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Application Software Development and Change Controls

Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and to ensure that different versions are not misidentified.

Such controls can prevent both errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Weaknesses in software program change controls were identified for 19 of the 21 agencies where such controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. At another, documentation was not retained to demonstrate user testing and acceptance.

- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs was prevented or detected.

- Agencies' policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or
- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a combination of physical and logical access controls and by effective supervisory review.

Segregation of duties was evaluated at 20 of the 24 agencies covered by our analysis, and weaknesses were identified at 17 of these agencies. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff involved with

procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt recorded by the same individual.

Operating System Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosures. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them.

Operating system software controls were covered in audits for 18 of the 24 agencies included in our review. This was double that of 1998, when this important control area had been reviewed for only nine agencies.

Weaknesses were identified at each of the 18 agencies for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Service Continuity

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location.

Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity controls were evaluated for 21 of the 24 agencies included in our analysis. Of these 21, weaknesses were reported for 20 agencies. Examples of weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.

- Disaster recovery plans were not fully tested to identify their weaknesses. At one agency, periodic walkthroughs or unannounced tests of the disaster recovery plan had not been performed. Conducting these types of tests provides a scenario more likely to be encountered in the event of an actual disaster.

In conclusion, the expanded body of audit evidence that has become available in the past 2 years on the status of federal information security shows that important operations at every major federal agency continue to be at risk as a result of weak information security controls. There are many specific causes of these weaknesses, but an underlying problem is poor security program management and poor administration of available control techniques. While agencies have taken steps to address problems and many have good remedial efforts underway, audits completed over the past year show that agencies by and large have not implemented the fundamental management practices needed to ensure that their computer-based controls remain effective on an ongoing basis.

The audit reports cited in the report being released today include many recommendations to individual agencies that address the specific weaknesses reported. For this reason, we are making no additional recommendations at this time. However, we have issued two executive guides that discuss practices that leading organizations have employed to strengthen the effectiveness of their security programs. These guides are *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998) and *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33, November 1999).

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

Contact and Acknowledgments

If you should have any questions about this testimony, please contact me at (202) 512-6253 or Robert Dacey at (202) 512-3317. We can also be reached by e-mail at *willemssenj.aimd@gao.gov* and *daceyr.aimd@gao.gov*, respectively.

(512027)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)